EXHIBIT D

What Is Network Policy?

Network policy is a collection of rules that govern the behaviors of network devices. Just as a federal or central government may lay down policies for state or districts to follow to achieve national objectives, network administrators define policies for network devices to follow to achieve business objectives.

Watch video (3:01) Explore policy solution

Benefits of network policy

A network that runs on policies can be automated more easily and therefore respond more quickly to changing needs. Many common tasks, such as adding devices and users and inserting new applications and services, can now be easily accomplished. Well-defined policies can benefit a network in the following ways:

- Align the network with business needs
- Provide consistent services across the entire infrastructure
- Bring agility through greater automation
- Make performance dependable and verifiable

An even bigger advantage to enterprises is the security gains from policy. By granularly defining policies that give users and devices the least amount of access to resources that they need to do their jobs, you can better protect sensitive data. Violations can be caught and mitigated quickly. Such zero-trust security measures reduce risk, contain threats, stop lateral movement of malware, and help verify regulatory compliance.

Why is it important for a network to follow policies?

A network that follows well-defined policies capably fills business needs that it is designed to support. Think of network policies as objectives or goals. Without clear objectives, your network can't be set up to deliver optimally, and without goals, its performance can't be measured.

Business intent and agility

Network policies reflect business intent. Network controllers ingest business intent and create policies that help achieve the desired business outcomes. Policies are enforced and carried out by network equipment such as switches, routers, wireless access points, and wireless LAN controllers. Networks operated in an ad hoc fashion, without guiding policies, will likely fail to deliver optimally.

Consistency of experience

Well-executed policies in the network provide consistency of service throughout it, regardless of locations, means of connectivity, or devices in use. This means users and things can use the network from anywhere and still have the same access privileges and quality of network experience.

Network automation	Network devices and their operations can be better automated when guidance exists. With policies, configurations can be automated and orchestrated so that each device does what's required to achieve the larger objectives.
Performance monitoring	Once well-understood goals are defined, metrics can be established to measure how the network is delivering. Continuous analysis of performance helps ensure that policies are being followed and business objectives are being met.
Network security	With policies in place, any violations can be easier to detect. Security is more easily enforced, threats more quickly contained, and risk rapidly reduced with security-related policies.

What do policies govern?

Policies don't exist in a vacuum. All network devices, users, and applications should be governed by those policies.

- Users - Effective policies need to recognize all types of users. Clearly, an admin user should have different rights and be able to do a wider array of tasks on the network than a guest user. Likewise, a financial user needs access to business-critical financial data, while a security guard does not.
- User and IoT devices - Access privileges provided to devices form key policies, especially as IoT expands. A policy could enable people to perform more tasks and access more types of information than a connected temperature sensor or printer. In fact, policies should expressly prohibit a moisture sensor from accessing a financial database.
- Applications - Not all applications are equal, and policies should reflect that. Bandwidth is always limited, so polices should prioritize traffic from business-critical applications over traffic from social media, for example.
- Data Type - Similarly, not all data types are of equal importance. Critical financial data demands a more restrictive policy. Video traffic may demand a specific quality-of-service (QoS) policy to help optimize performance levels.
- Location - Location can be an important policy attribute. As telecommuting becomes more widespread, users' locations may affect their security profiles and what applications and data they can access. For example, a user may access a human resources data base from the privacy of their home office, but not while working from a public coffee shop.

What are different kinds of network policies?

Since network policies specify how the network must function in different circumstances, there is no set list of policies. A network's policies depend on what's necessary to achieve business objectives. Some of the more common policies that all businesses need to consider are:

Access and security	These govern whether a given user or thing will become part of the network and what resources the person or device can access. Access and security policies might be the most important types of policies, since the security of data and applications depends on them.
Application and QoS	These define the relative importance of various applications and how the traffic for each should be prioritized.
Traffic routing and service insertion	These govern how traffic from certain types of users should be routed, such as guest traffic through a firewall.

IP-based versus group- or role-based	Policies can be defined on an IP-address level or by role. Role-based policies are dynamic, offer more flexibility, are easier to automate, and support user and device mobility. IP-based policies are static, do not scale, and are best suited for an environment that doesn't change much.

Why has it been difficult to enforce network policies?

Despite the acknowledged importance of setting and adhering to policies, most corporate networks do not have effective policy strategies in place. The reasons most often cited are:

Ad hoc growth	Many enterprise networks simply evolve over the years. New divisions and their needs are addressed in a one-off manner. Each merger or acquisition bridges two disparate networks without an effective plan. Several types of network devices with varying capabilities may also contribute to disorder.
Difficulty of specifying or updating policies	Even if the network was well designed originally, operating policies may not have been adjusted as business needs changed over the years. In these cases, there's often no good way to update or specify new policies without redesigning the entire network.
Traditional manual IP-based processes that don't scale and aren't agile	When network administrators must adapt their networks to new business needs, they may be constrained by the need to manually reconfigure network devices. This lack of agility and the scaling difficulties mean network cannot live up to expectations.

What does it take to implement effective policies?

Of course, you can't implement policies without knowing what policies to implement. This is particularly true for larger networks that have evolved over time and whose administrators may not have a complete grasp of business needs and how the network is responding to them. Here are the steps for implementing policies that work:

1. Identify - Figure out who and what is on the network. Users may have brought their own devices, and departments may have plugged in IoT devices without administrator knowledge. Without an inventory of devices, and their security postures (locations, operating systems, latest software patches and updates, etc.), it's difficult to set policies that govern their uses and places in the network.
2. Visualize - Understand how users and devices communicate. If you're starting from scratch, you can preplan, but you don't always have that luxury.
3. Define - Once you have a solid idea of how your network is being used, you can start to define policies that will permit, deny, or modify those flows.
4. Model - After visualizing and defining your policies but before putting them in place, do a "dry run" to determine what effects the policies will have on users, traffic, and performance.
5. Activate - Here, you activate network devices to enforce policies as per the functions they perform.
6. Extend - Sometimes, activating policies in just one network isn't enough. In this age of connectedness, consistent policies must permeate all networks within the enterprise – campus, branch, WAN, and data center, as well as the ecosystem, such as ITSM. Extending policies would make all networks collaborate to fulfill business intent.
7. Assure - It's not enough to define, model, and activate policies. You need to help ensure that they're being followed and getting the job done. Here, you analyze the network and evaluate whether it is enforcing the policies and identify any fine-tuning you may need to do.

How can policies be defined and enforced in a modern network?

All the tasks listed above for discovering, defining, authoring, and activating policies are certainly not easy to perform. Network controllers that follow the industry's intent-based networking (IBN) framework are best suited for those jobs. They take business intent as input, translate it into policies, and make sure the policies are being applied appropriately and delivering the desired results.

Deploy network policy

Cisco Catalyst Center
Manage SD-Access with a central dashboard across the entire network.

Identity Services Engine (ISE)
Simplify delivery of identity-based policy for users and devices.

Cisco networking software
Easily buy, manage, and upgrade your network and infrastructure software.

Resources

Intent-Based Networking

Network Control for the Digital Age

Creating More Agile and Upgradeable Networks with a Controller-Based Architecture

Policy-based networking

Policy products and solutions

Cisco Networking

Cisco Software-Defined Access

Cisco Identity Services Engine

Intent-based network controllers

Cisco Catalyst Center

Cisco Catalyst SD-WAN Manager

Cisco Application Policy Infrastructure Controller (APIC)

Related networking topics

Managed Switches Versus Unmanaged Switches

What Is Network Provisioning?

What Is Network Monitoring?

What Is a User Authentication Policy?

What Is Network Security Policy Management?

What Is Software-Defined Access?

What Is Network Security?

What Is a Network Controller?

What Is Network Segmentation?

What Is a Network Fabric?